

WHAT IS CLAIMED IS:

1. A management system of a public key certificate comprising: a service provider which verifies validity of a presented public key certificate and, if the verification can correctly be made, provides a service; a certificate authority on which said service provider relies; and a smart card, wherein
said smart card comprises:
a storing unit which stores
a first private key and a first public key making a pair together therewith which are necessary to issue a certificate to said certificate authority, a first certificate issued for said first public key,
a second private key and a second public key making a pair together therewith which are generated to receive a service from said service provider, and
a second certificate which is issued for said second public key by said certificate authority on which said service provider relies; and
a key generating unit which generates said first and second public keys and said first and second private keys,
said certificate authority comprises:
a storing unit which stores a third private key for generating a certificate of said second public key for said smart card and said certificate which is issued to a third public key making a pair together with said third private key; and

a certificate generating unit which generates the second certificate for said second public key on the basis of an issuing request, and

said smart card comprises a certificate generating unit which issues the certificate of said certificate authority by using said stored first private key on the basis of an issuing request for the certificate from said certificate authority.

2. A system according to claim 1, wherein

said certificate authority comprises:

a revocation information generating unit for generating revocation information of the certificate on the basis of a revoking request for the certificate; and

a revocation information database for storing the revocation information generated by said revocation information generating unit,

said smart card presents said first and second certificates to said service provider in order to receive the service from said service provider, and

said service provider comprises a certificate verifying unit for inquiring of said certificate authority about the revocation information of said first and second certificates when the validity of said presented first and second certificates is verified.

3. A system according to claim 1, wherein

said smart card

constructs said storing unit as an area which

is specific to said service provider and

includes a service provider authenticating unit for permitting only said service provider corresponding to said specific area to access said specific area.

4. A system according to claim 1, wherein said service provider specific area of said smart card and data stored in said certificate generating unit have been encrypted.

5. A system according to claim 1, further comprising
a certificate validation authority, and
said certificate validation authority making validity verification of the certificate by said certificate verifying unit of said service provider as an alternative of said service provider.

6. A system according to claim 1, further comprising
a certificate storage authority, and
said certificate storage authority holding a plurality of certificates stored in said smart card as an alternative of said smart card and providing said certificate in accordance with a request.

7. A system according to claim 2, wherein
when said certificate authority verifies said second certificate, said service provider transmits a challenge to said smart card,
said smart card

encrypts said challenge by said second private key and transmits said encrypted challenge, the second certificate corresponding to said second private key, and the first certificate corresponding to said first private key to said service provider,

said service provider comprises:

a certificate verifying unit for decrypting said encrypted challenge, confirming whether the decrypted challenge coincides with said challenge transmitted to said smart card, obtaining the revocation information of said received first and second certificates, and executing the verifying process of said first and second certificates by using said obtained revocation information; and

a service providing unit for providing the services in response to a decision indicating that said first and second certificates are valid in said verifying process.

8. A system according to claim 7, wherein said smart card

constructs said storing unit as an area specific to said service provider and,

when said service provider transmits and receives data to/from said service provider specific area,

said service provider executes a mutual authenticating process between said service provider and said service provider specific area.

9. A system according to claim 7, wherein
when data is stored into said service
provider specific area of said smart card and into said
certificate generating unit, said data is encrypted and
thereafter stored.